

How to Configure Link Protection for Mail Security in the Firewall

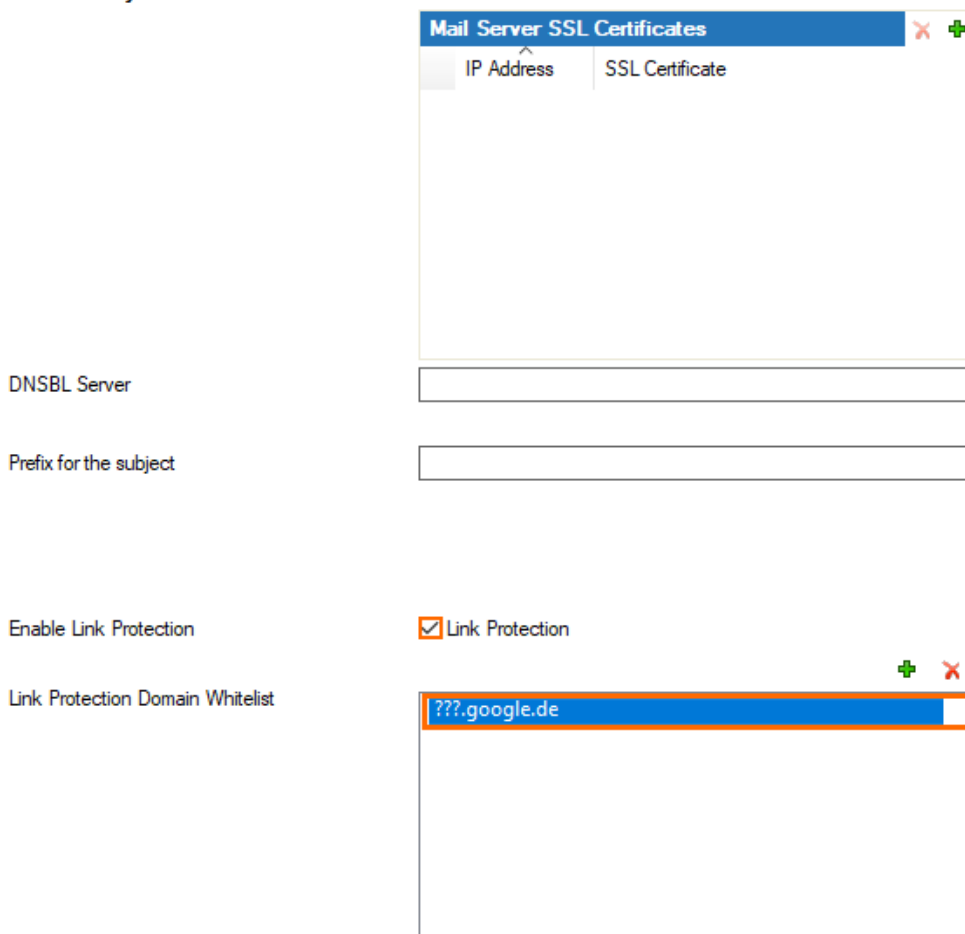
<https://campus.barracuda.com/doc/79463042/>

Link Protection protects users from fraudulent links inside of plain-text and HTML emails. This cloud-based service requires an active Advanced Threat Protection (ATP) subscription.

Step 1. Activate Link Protection Globally on the Firewall

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Security Policy.**
2. Click **Lock.**
3. In the **Mail Security** section, enable Link Protection:
 - **Enable Link Protection** – Select the check box **Link Protection.**
 - **Link Protection Domain Whitelist** – Enter the domain names you want to exclude from being evaluated by Link Protection. The wildcards * and ? are allowed.

Mail Security



The screenshot shows the Mail Security configuration page. At the top, there is a 'Mail Server SSL Certificates' window with columns for 'IP Address' and 'SSL Certificate'. Below this are input fields for 'DNSBL Server' and 'Prefix for the subject'. The 'Enable Link Protection' section has a checked checkbox for 'Link Protection'. The 'Link Protection Domain Whitelist' section has a text input field containing '???google.de'.

4. Click **Send Changes** and **Activate.**

Step 2. Create a Dst NAT Access Rule to Forward Mail Traffic to the Mail Server

A **Dst NAT** access rule redirects SMTP traffic sent to an external IP address to a destination on the internal network.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (+) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.

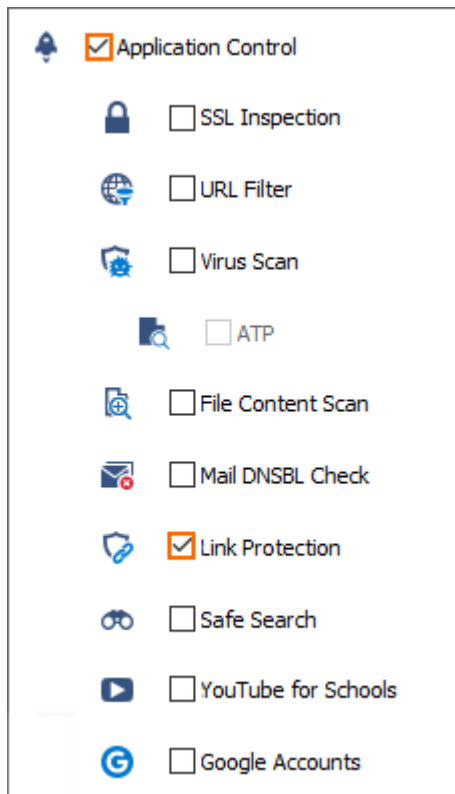


4. Select **Dst NAT** as the action.
5. Enter a **Name** for the rule. For example, Mail - Server.
6. Specify the following settings that must be matched by the traffic to be handled by the access rule:
 - **Source** - The source addresses of the traffic.
 - **Destination** - The destination addresses of the traffic.
 - **Service** - Select **SMTP**.
 - **Target List** - Enter the internal IP of your mail server.
 - **Connection Method** - For more information, see [Connection Objects](#).

<input type="checkbox"/> Dst NAT		Mail-Server	
<input type="checkbox"/> Bi-Directional		<input type="checkbox"/> Dynamic Rule	
<input type="checkbox"/> Deactivate Rule			
Source VR Instance default		Destination VR Instance Same as Source	
Source Internet Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16	Service SMTP TCP 25 mail-smtp Report if other...	Destination ADC-WAN-EXTERNAL 62.99.0.42	
		Redirection Target List <input type="checkbox"/> Reference: 10.0.10.1 Fallback List of Critical Ports	
Authenticated User Any	Policies IPS Policy Default Policy Application Policy AppControl, URL.Fil SSL Inspection Policy N.A. Schedule Always QoS Band (Fwd) No-Shaping QoS Band (Reply) Like-Fwd		Connection Method Original Source IP Original Source IP (same port)
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

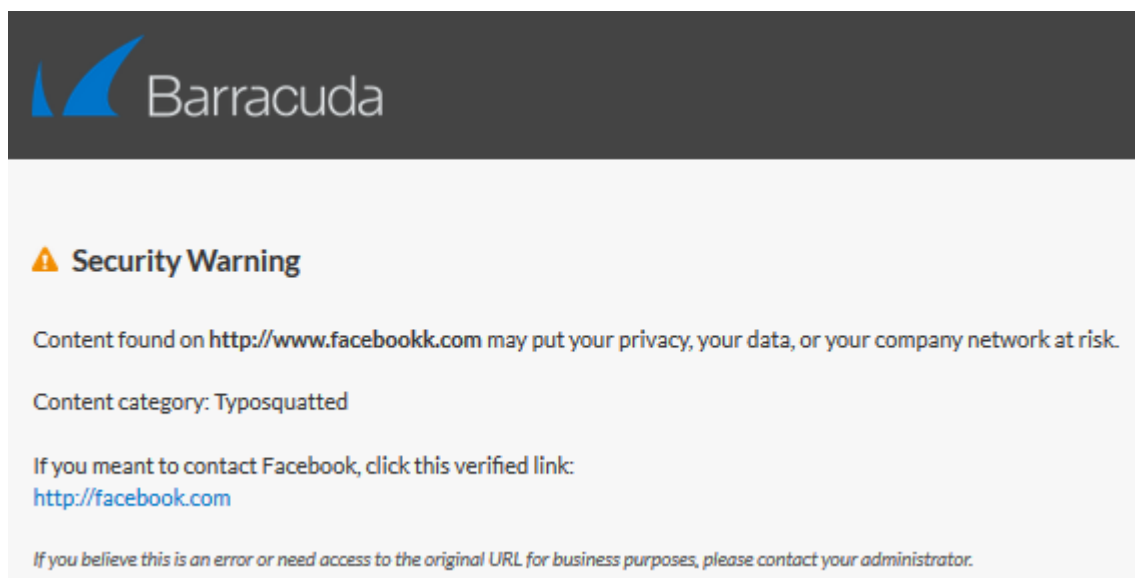
7. In **Application Policy**:

- **Application Control** - Select the check box. For more information on all Application Control features, see [Application Control](#).
- **Link Protection** - Select the check box.



8. Click **OK**.
9. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located *above* the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.
10. Click **Send Changes** and **Activate**.

Your firewall is now configured to handle embedded WEB-links inside of plain-text and HTML emails. In case Link Protection detects a fraudulent URL, you will be redirected to a Security Warning page that will show up in your web browser, i.e.:



Figures

1. activate_globally_lp_01.png
2. FW_Rule_Add_01.png
3. add_access_rule_redirect_01.png
4. enable_application_rule_for_lp_01.png
5. securit_warning_page_01.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.